It is claimed:

1. A method for handling on a wireless mobile communication device a secure message to be sent to a recipient, comprising the steps of:

receiving data about a security key associated with the recipient;

using the received data to perform a validity check with respect to using the message recipient's security key to send a secure message to the recipient;

wherein an issue exists due to the validity check;

determining a reason for the validity check issue;

wherein the reason for the validity check issue is provided to the mobile device's user.

2. The method of claim 1, wherein a message is provided to the user indicating the reason that a problem exists with respect to sending a secure message to the recipient in addition to indicating the reason related to the problem.

3. The method of claim 1, further comprising the step of allowing the user to resolve the validity check issue through use of the information provided in the validity check reason, wherein the secure message is sent after resolution of the validity check issue by the user.

4. The method of claim 1, wherein the security key is a public key, wherein a user composes a secure message, wherein the composed message is to be encrypted using the recipient's public key.

5. The method of claim 4, further comprising the steps of:

creating a list of all of the recipients for the outgoing message;

receiving data about the recipients' public keys that includes certificate information associated with the recipients;

performing the validity check with respect to the certificate information associated with the recipients.

6. The method of claim 1, further comprising the steps of:

determining whether a certificate for a recipient can be located;

providing as a validity check reason that an intended message recipient's certificate was not located.

7. The method of claim 6, wherein the user is allowed to remove a recipient whose certificate was not located before sending a secure message to another recipient.

8. The method of claim 6, wherein the user is allowed to cancel sending the message to a recipient whose certificate was not located.

9. The method of claim 6, further comprising the step of:

determining whether the certificate for a recipient is locally available on the mobile device.

10. The method of claim 6, further comprising the step of:

determining whether the certificate for a recipient is remotely available.

11. The method of claim 6, further comprising the step of collating certificates that correspond to the recipients before performing the validity check.

12. The method of claim 6, wherein the message is to be encrypted using a Secure Multipurpose Internet Mail Extensions (S/MIME) scheme or a Pretty Good Privacy PGP scheme.

13. The method of claim 1, wherein the received data about a recipient's security key includes whether a recipient's certificate is permitted to be used;

wherein the validity check issue indicates that the recipient's certificate is not permitted to be used.

14. The method of claim 13, wherein the data about permission whether to use a recipient's certification is based on a usage field contained in the certificate.

15. The method of claim 13, wherein the data about permission whether to use a recipient's certification is based on a control file installed on the mobile device that specifies which certifications are allowed to be used.

16. The method of claim 1, wherein the issue involves a validity check failure, said method

further comprising the step of providing the reason of the validity check failure to the mobile device's user.

17. The method of claim 1, wherein the received data about a recipient's security key includes strength of the recipient's certificate;

wherein the validity check issue is directed to whether the recipient's certificate is permitted to be used based upon the strength of the recipient's certificate.

18. The method of claim 1, wherein the received data about a recipient's security key includes whether the recipient's certificate is trusted, wherein decision to include a recipient for a secure message is based upon whether the recipient's certificate is trusted.

19. The method of claim 1, wherein the received data about a recipient's security key includes validity and revocation status of a recipient's certificate, wherein decision to include a recipient for a secure message is based upon the validity and revocation status of a recipient's certificate.

20. The method of claim 1, wherein the mobile device's user decides to send the message to a recipient despite being notified of the validity check issue.

21. The method of claim 1, wherein means for providing a wireless network and means for providing a message server are used to transmit the secure message from the mobile device.

22. The method of claim 1, wherein the mobile device is a handheld wireless mobile communications device or a personal digital assistant (PDA).

23. A data signal that is transmitted using a communication channel, wherein the data signal includes the secure message of claim 1;

wherein the communication channel is a network, wherein the data signal is packetized data that is transmitted through a carrier wave across the network.

24. Computer-readable medium capable of causing the mobile device to perform the method of claim 1.

25. An apparatus for handling on an electronic device a secure message to be sent to a recipient, comprising:

a secure message processing module for use with a messaging client that sends electronic messages to recipients;

wherein the secure message processing module receives data about a security key associated with the recipient;

wherein the secure message processing module uses the received data to perform a validity check with respect to using the message recipient's security key to send a secure message to the recipient;

wherein an issue exists based upon the validity check and a reason is determined for the validity check issue;

wherein the secure message processing module provides the reason of the validity check issue to the electronic device's user.

26. A wireless mobile communication device that handles a secure message to be sent to a recipient, comprising:

a certificate store to store certificate data;

means for using the stored certificate data to perform a validity check with respect to using the message recipient's security key for sending a secure message to the recipient;

wherein an issue exists due to the validity check;

means for determining a reason for the validity check issue;

means for providing the reason of the validity check issue to the mobile device's user.